View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

JOURNAL OF ALGEBRA **148**, 325–336 (1992)

On Bounds for Groups of Multipliers of Planar Difference Sets

CHAT YIN HO*

Department of Mathematics, University of Florida, Gainesville, Florida 32611

Communicated by Walter Feit

Received October 9, 1990

COMMEMORATING THE SIXTIETH BIRTHDAY OF PROFESSOR J. G. THOMPSON

1. INTRODUCTION

A subset D of a group S is a planar difference set if for each nonidentity element z of S there exists a unique pair $x, y \in D$ such that $z = xy^{-1}$; also there exists a unique pair $c, d \in D$ such that $z = c^{-1}d$. The study of a planar difference set of a finite group S is equivalent to the study of a finite projective plane Π admitting a regular collineation group isomorphic to S. (See, for example, [L or HP].) The latter leads to the study of multipliers. Here an automorphism of the regular collineation group S is a multiplier if it is also a collineation of Π. The set of all multipliers of Π is called the multiplier group of Π and S is called a Singer group of Π. In this paper we prove the following.

THEOREM 1. *Suppose the multiplier group contains an involution α. Then the order of the projective plane is a square, and $S = A \cdot B$, where $A = [S, \alpha] = \{s \in S \mid s^\alpha = s^{-1}\}$ is an abelian Hall subgroup of order $n - \sqrt{n} + 1$, which is also an arc (i.e., no three points of A are collinear), and $B = C_S(\alpha)$ is a Hall subgroup of order $n + \sqrt{n} + 1$, which is also a Baer subplane.*

THEOREM 2. *Let M be an abelian group of multipliers of a projective plane of order n. Then the following holds:*

(1) *Either $|M| \leqslant n + 1$ or n is a square.*

(2) *Assume the following hypothesis holds: the multiplier group of any*

* Partially supported by NSA Grant MDA904-90-H-1013.

0021-8693/92 $5.00

Copyright © 1992 by Academic Press, Inc.
All rights of reproduction in any form reserved.

projective plane of square order has a central involution. Then $|M| \leqslant n+1$ *except* $n=4$.

(3) *If the regular collineation group is abelian, then* $|M| \leqslant n+1$ *except* $n=4$.

For cyclic planes (i.e., projective planes admitting cyclic Singer groups) we prove the following.

THEOREM 3. *Let* M *be a group of multipliers of a cyclic plane of order* n. *Let* $v(n)=n^2+n+1$. *Then the following holds:*

(1) *We have* $|M| \leqslant n+1$ *except for* $n=4$. *if* M *does not contain any planar collineation, then* M *is cyclic of odd order and* $|M|$ *divides* $n-j$, *where* $j \in \{-1, 0, 1\}$ *such that* $n \equiv j \pmod 3$.

(2) *If* $|M|=n+1$, *then* n *is even and* v *is a prime.*

(3) *If* $|M|=n$, *then* $3 \mid n$, *and* n *is odd, and* v *is a prime.*

(4) *If* $1 \neq M$, *then* $|M| \neq n-1$.

(5) *If* $1 \neq M$, *then* $|M|=n-2$ *if and only if* $n=5$.

(6) *If* $1 \neq M$, *then* $|M|=n-3$ *if and only if* $n=9$.

Some remarks are in order. The reason for assuming the hypothesis in Theorem 2.(2) is the lack of Hall's multiplier theorem for non-abelian Singer groups. Projective planes of order 2 or 8 show that the bound $n+1$ is attained. Note that in a projective plane of order 4, the multiplier group has order $6<4+1$. In all known examples, for projective planes of order n, $|M|=n+1$ (resp. $|M|=n$) if and only if $n=2$ or 8 (resp. $n=3$).

The multiplier group of a Desarguesian plane of order 81 has order $3 \cdot 4=12>\sqrt{81}$. This shows that $\sqrt{n}$ is not a bound for the order of a multiplier group. Theorem 2 also yields a bound, $(n+1)/3$, for odd-order groups of multipliers, which are planar but not triangular, of abelian Singer groups.

For $n \in \{3673=53 \cdot 71,\ 3869=53 \cdot 73,\ 4189=59 \cdot 71\}$, the multiplicative order of 71 (resp. 71, 73) modulo $v(n)$ is strictly bigger than $n+1$. Therefore, projective planes with abelian Singer groups of the corresponding orders cannot exist by Theorem 2. Note that these orders are larger than 3600, which is the upper bound of the orders being verified by V. K. Keiser [D, p. 209] for the conjecture that finite cyclic planes have prime power order. Observe also that for these values of n, $v(n)$ is not a prime. In fact, $v(n)$ is divisible by 3, 31, and 3, respectively.

Feit [F] and Kantor [K] prove that a flag-transitive projective plane of order n is Desarguesian, or it is a cyclic plane such that $v(n)$ is a prime, the multiplier group has order $n+1$, $8 \mid n$ and n is not a power of 2. Theorem 3 (2) is in the same spirit but from the multiplier group's point of view. All the extra conclusions on n also hold here.

In the proof of Theorem 3, we obtain that if $1 \neq |M| \in \{n-3, n-2, n, n+1\}$ then M is the multiplier group. Theorem 3 (5), (6), together with results in [Ho] and [HoP] characterize projective planes of order 2, 3, 4, 5, 8, or 9 in terms of the orders of their multiplier groups.

For cyclic planes of order n such that M does not contain any planar element, we prove the following results in Section 5. If $|M| > (n+1)/2$, then $|M| = n+1$ or n (5.3). If $|M| = n-k$ for some $k \geqslant 1$, then $n \leqslant 2k+1$ (5.4). Further, if $1 \leqslant k \leqslant 10$, then $k = 2$, 4, 8, and 10, and the corresponding value of n is 5, 7, 11, and 13 (5.5).

2. Proof of Theorem 1 and Some Preliminary Results

In this section, Π is a finite projective plane of order n with a Singer group S (i.e., collineation group which acts regularly on the points of Π). We call Π an abelian (resp. cyclic) plane if S is abelian (resp. cyclic). We sometimes identify the points of Π with the elements of S. For any number x, define $v(x) = x^2 + x + 1$. Let $v = v(n)$ and G be the full collineation group of Π. A multiplier of Π is an automorphism of S which is also a collineation. For $H \subseteq G$, let $P(H)$ (resp. $L(H)$) be the set of fixed points (resp. lines) of H and Fix (H) be the fixed-point-line substructure of H. An integer t is called a numerical multiplier if the automorphism of $S: s \to s^t$ is a multiplier of Π. We denote this automorphism by $m(t)$. Our terminology in group theory is taken from [G], that of projective planes is taken from [HP], and that of difference sets is taken from [B or L].

Lemma 2.1. *A nontrivial multiplier cannot be a perspectivity.*

Proof. Let $1 \neq \alpha$ be a multiplier. Suppose α is perspectivity. There is $\sigma \in S$ such that $1 \neq [\alpha, \sigma] = \beta$. Since $\beta = \alpha^{-1}\alpha^{\sigma}$ is a product of two perspectivities, it fixes at least one point. This contradicts the fact that S acts regularly on the points of Π. The proof of the lemma is complete.

2.2. *Proof of Theorem* 1. Suppose the multipleir group M contains an involution α. By Lemma 2.1, the involution α is a Baer involution. Hence n is a square and $B = C_S(\alpha)$ is a Baer subplane. Since $v(n)$ is odd, S is solvable by Feit–Thompson theorem [FT]. As $v(n) = v(\sqrt{n})\, v(\sqrt{n}-1)$ and $(v(\sqrt{n}),\ v(\sqrt{n}-1)) = 1$ (see, for example, [Ho 1, 2.2]), S has an α-invariant Hall subgroup A with $|A| = v(\sqrt{n}-1)$. Since $|B| = v(\sqrt{n})$, $(|A|, |B|) = 1$. So $S = AB = BA$ and $A \cap B = 1$. This implies that $C_A(\alpha) = 1$. Thus α inverts each element of A. So A is abelian and $A = \{s \in S \mid s^{\alpha} = s^{-1}\}$ (see, for example, [H, pp. 24, 14]). Threfore $A = [A, \alpha]$. Since $S = B \cdot A$ and $B = C_S(\alpha)$, $[S, \alpha] = [A, \alpha] = A$.

We now prove that A is an arc. For each element $s \in S$, $s = s_A s_B$, where $s_A \in A$ and $s_B \in B$ are uniquely determined. There is a difference set D invariant under α (see, for example, [L, p. 208, Theorem 2.17]). Let $x, y \in D$. We claim that if $x_B = y_B$, then either $x = y$ or $x = y^\alpha$. Assume $x_B = y_B$. Then $xy^{-1} \in A$. Since $A = \{s \in S \mid s^\alpha = s^{-1}\}$, $x^\alpha (y^\alpha)^{-1} = (xy^{-1})^\alpha = (xy^{-1})^{-1} = yx^{-1}$. As x, y, x^α, y^α all belong to D, the definition of planar difference set implies that either $x = y$ or $x = y^\alpha$ as claimed.

Let Ds be any line of Π. If xs, $ys \in Ds \cap A$, then $xy^{-1} = (xs)(ys)^{-1} \in A$. Let $xy^{-1} = a \in A$. Thus, $x = ay$. Hence $x_A x_B = a y_A y_B$. As $a y_A \in A$, the last equality and the uniqueness of the factorization of an element of $s \in S$ into $s_A s_B$ imply that $x_B = y_B$. Hence, either $x = y$ or $x = y^\alpha$. Therefore $|Ds \cap A| \leqslant 2$. This proves that A is an arc.

The author thanks Blokhuis for informing him that in the Desarguesian case, it is known that A is an arc. The next two results concern the geometry of subgroups of S.

LEMMA 2.3. *Let H be a subset of S. If there exists a line l such that $3 < |H \cap l| = |H|$ or $|H| - 1$, then H cannot be a subgroup of S.*

Proof. By way of contradiction, assume that H is a subgroup. Let $h \in H \cap l$. Since $3 < |H|$ and at most one point in H is outside l, there is $1 \neq r \in H$ such that $hr \in l$. If $(hr) r \in l$, then the line lr contains two distinct points hr, $(hr) r$ of l. This implies that $lr = l$, which contradicts the regularity of S. Hence, $(hr) r \notin l$.

Let $P = hr$. Since $3 < |H|$, there is $1 \neq s \in H$ such that $s \neq r$. Thus, $Ps \neq Pr$. Now Pr is the only point in H outside l and $Ps \in H$ as H is a subgroup. This implies that $Ps \in l$. Suppose $(Ps) s \in l$. Then the line ls contains two distinct points: Ps and $(Ps) s$ of l. This implies that s fixes the line l, a contradiction. Therefore $(Ps) s \notin l$. So $(Ps) s = Pr$. Since $3 < |H|$, there is $1 \neq t \in H$ such that $r \neq t \neq s$. As $r \neq t$, $Pr \neq Pt$. So $Pt \in l$. From $t \neq s$, we obtain $Ps \neq Pt$. If $(Ps) t \notin l$, then $(Ps) t = (Ps) s$ is the unique point in H outside l. However, this implies that $t = s$ as S is regular. This contradiction proves that $(Ps) t \in l$. Therefore ls contains two distinct points Pt, $(Ps) t$ of l, which implies $ls = l$. This final contradiction proves the lemma.

COROLLARY 2.4. *Suppose U is a group of multipliers. Then $P(U) = C_S(U)$. If $P(U) \neq 1$, then* Fix(U) *is a triangle or a subplane.*

Proof. Suppose $P(U) \neq 1$. If $|P(U)| = 3$, then $P(U)$ is a Sylow 3-subgroup of S as 9 does not divide $v(n)$. Since $P(U) u = P(U)$ for any $1 \neq u \in P(U)$, the regularity of S implies that $P(U)$ cannot be collinear. So Fix(U) is a triangle in this case. The rest of the proof now follows from 2.3 and the fact that Fix(U) is a closed substructure.

In the rest of this section we assume that S is abelian and D is a difference set invariant under M. Let $j \in \{-1, 0, 1\}$ such that $n \equiv j \pmod 3$. Then the number of fixed points of $m(n)$ on D is $j+1$. Let $\Omega = D \backslash P(m(n))$. Then $|\Omega| = n - j$ and $\Omega^M = \Omega$.

PROPOSITION 2.5. *Suppose S and M are both abelian. If M does not contain any planar element, then M is cyclic of odd order and acts semi-regularly on Ω. In particular, $|M|$ divides $n-j$.*

Proof. Since any involution of M is a Baer involution by Lemma 2.1, $|M|$ is odd. Suppose M is not cyclic. Then M contains a subgroup $H \cong Z_p \times Z_p$ for some prime p as M is abelian. Hence, $S = \prod_{1 \neq h \in H} C_S(h)$. As $v = v(n)$ is not divisible by 9, the Sylow 3-subgroup of S has order 1 or 3. This implies that there is $h \in H$ such that $1 \neq C_S(h)$ and $|C_S(h)| \neq 3$. Thus h is planar by Corollary 2.4. This contradiction proves that M is cyclic.

Next we prove that M acts fixed-point-freely on Ω. Let $m \in M$, and let $\Gamma = C_\Omega(m)$. Suppose $\Gamma \neq \phi$. Since $m(n)$ has no fixed point on Ω, so $3 \mid |\Gamma|$. As $C_S(m(n))$ contains the Sylow 3-subgroup T of S, $T \cap \Omega = \phi$. Therefore $T \cap \Gamma = \phi$. Since $C_S(m)$ is a subgroup containing Γ, the last equality shows that $|C_S(m)| \neq 3$. This implies that m is planar by Lemma 2.1 and Corollary 2.4. This contradiction proves that $\Gamma = \phi$. So M acts fixed-point-freely on Ω. Since M is abelian, this implies that M is semi-regular on Ω. Therefore, $|M|$ divides $|\Omega| = n - j$.

LEMMA 2.6. *Suppose S is abelian. If n is even and $n \equiv 1 \pmod 3$, then n is a square.*

Proof. Since $n \equiv 1 \pmod 3$ and v is not divisible by 9, the Sylow 3-subgroup T of S has order 3. Now 2 is a numerical multiplier as n is even. The restriction of $m((2))$ on T has order 2. Hence n is a square by Lemma 2.1.

3. THEOREM 2

We continue to use the notations in the last section. Let M be a group of multipliers of Π and let S be a Singer group normalized by M. For the reader's convenience we record the following known result.

THEOREM 3.1. (Hall [HP]). *If S is abelian then any divisor of n is a multiplier.*

LEMMA 3.2. *Numerical multipliers are in the center of the multiplier group.*

Proof. This follows from the definitions.

3.3 *Proof of Theorem* 2. We apply induction on $|M|$ and n to prove Theorem 2.

(1) Proof of Theorem 2(1). If $|M|$ is even, then n is a square by Theorem 1. Therefore, we may assume $|M|$ is odd. Since a finite group of order $v(9) = 7 \cdot 13$ is cyclic, projective planes of order less than or equal to 9 are cyclic planes, and so they are Desarguesian and satisfy the conclusion of Theorem 2(1). Therefore, we may assume the following holds.

(3.1) $n > 9$.

If M has a regular point orbit on any line, then $|M| \leqslant n+1$. Therefore, we may also assume the following holds.

(3.2) A line fixed by M cannot contain any regular point orbit of M. There is a faithful point orbit of M. (See, for example, [D] or [HP]). Since M is abelian, this is a regular orbit. First suppose $\mathrm{Fix}(M)$ is a triangle or a subplane. Let $\{A, B, C\}$ be a triangle in $P(M)$. Let X be a point in a regular orbit of M. By (3.2), CX, BX are lines not fixed by M. Since $CX \cap BX = X$, $M_{CX} \cap M_{BX} \subseteq M_X$. But $M_X = 1$, so $M_{CX} \cap M_{BX} = 1$. This implies that $|M| \geqslant |M_{CX} M_{BX}| = |M_{CX}|\,|M_{BX}|$ as $M_{CX} M_{BX}$ is a subgroup in the abelian group M. Hence, one of the order of these two subgroups (say, $|M_{BX}|$) is less than or equal to $\sqrt{|M|}$. For any point Y, let $[Y]$ denote the set of lines incident with Y. Now $(BX)^M \subseteq [B]^M = [B]$. Hence $|(BX)^M| \leqslant n-1$ as $BX \neq BC$ or AB by (3.2). On the other hand, $|(BX)^M| = |M|/|M_{BX}|$. If $M_{BX} = 1$, then $|M| = |(BX)^M| \leqslant n-1$, and Theorem 2(1) holds. Suppose $M_{BX} \neq 1$. Since $L(M) \cup \{BX\} \subseteq L(M_{BX})$, $\mathrm{Fix}(M_{BX})$ is a proper subplane Ω by Corollary 2.4. Let the order of this subplane be m. Since M is abelian, M acts on Ω. Thus $(BX)^M$ belongs to the set of lines of Ω which are incident with B and different from AB, BC. Therefore $|(BX)^M| \leqslant m-1$. As $|M_{BX}| \leqslant \sqrt{|M|}$, we have $|(BX)^M| = |M|/|M_{BX}| \geqslant \sqrt{|M|}$. On the other hand, $m \leqslant \sqrt{n}$ by a theorem of Bruck [HP, pp. 81]. Hence, we obtain $\sqrt{|M|} \leqslant |(BX)^M| \leqslant \sqrt{n} - 1$. This implies that $|M| < n$ and Theorem 2(1) holds.

Therefore, by Corollary 2.4, we may assume that $\mathrm{Fix}(M)$ consists of a point and a line. If $|P(\alpha)| = 3$ for some $\alpha \in M$, then $P(\alpha)$ is a Sylow 3-subgroup of S which is invariant under M as M is abelian. Since $|M|$ is odd, this implies that $P(\alpha) \subseteq \mathrm{Fix}(M)$. Hence, $\mathrm{Fix}(M)$ is a triangle or a subplane. This contradiction, along with Corollary 2.4, proves that the following holds in the present situation.

(3.3) If $\alpha \in M$ with $C_S(\alpha) \neq 1$, then α is planar.

Let $\mathrm{Fix}(M) = (P, l)$. For any point Y on l different from P, then $Y \neq Y^M$. By (3.2), Y^M is not a regular orbit of M. Hence, $M_Y \neq 1$. By (3.3) nontrivial elements of M_Y are planar. As $Y^M \subseteq l \cap \mathrm{Fix}\,(M_Y)$, we obtain the following.

(3.4) If $Y \in (l) \backslash P$, then $M_Y \neq 1$ and nontrivial elements in M_Y are planar. Further, $|Y^M| \leqslant y+1$, where y is the order of $\mathrm{Fix}(M_Y)$.

Among the nontrivial planar elements of M, choose α such that $|C_S(\alpha)|$ is maximum. Thus, the order m of $\mathrm{Fix}(\alpha)$ is maximal among the fixed subplanes of nontrivial elements of M. Let $K=\{\beta\in M \mid \mathrm{Fix}(\beta)=\mathrm{Fix}(\alpha)\}$. Since $l^\alpha=l$ and α is not a perspectivity, the set of points on l not fixed by α is not empty. Denote this set by Γ. Since M is abelian, M acts on $P(\alpha)\cap(l)$. Thus M also acts on Γ. Let $Q\in\Gamma$. Thus $Q^M\subseteq\Gamma$ and so $Q^M\cap P(\alpha)=\phi$. Since $P(\alpha)=P(\beta)$ for $\beta\in K$, K acts fixed-point-freely on Q^M. So $|K|\leqslant|Q^M|$. By (3.4), $1\neq M_Q$ is planar. Let the order of $\mathrm{Fix}(M_Q)$ be q. Since M is abelian, M acts on $\mathrm{Fix}(M_Q)$. So Q^M is a subset of $P(M_Q)\cap(l)$. In particular, $|Q^M|\leqslant q+1$. Therefore $|K|\leqslant q+1$.

As M induces an odd-order group of multipliers on $\mathrm{Fix}(\alpha)$, induction yields $|M/K|\leqslant m+1$. Hence $|M|=|M/K|\ |K|\leqslant(m+1)(q+1)$. Let H be the kernel of the action of M on $\mathrm{Fix}(M_Q)$. An element $h\in H\cap K$ will fix all points of $P(\alpha)\cap(l)$ and Q^M. If $h\neq 1$, this implies that h is planar and the order of $\mathrm{Fix}(h)$ is strictly bigger than m, which is impossible. This contradiction proves $H\cap K=1$. Hence, $|M|\geqslant|H|\,|K|$. So one of these two subgroups, say J, has order less than $\sqrt{|M|}$. From $|M/K|\leqslant m+1$ and $|M/H|\leqslant q+1$, we get $\sqrt{|M|}\leqslant|M/J|\leqslant r+1$, where $r=m$ or q. Suppose $r\neq\sqrt{n}$. Then $r^2+r\leqslant n$ by a theorem of Bruck [HP, p. 81]. So $r<\sqrt{n}$. Hence, $\sqrt{|M|}\leqslant r+1\leqslant\sqrt{n}$, and $|M|\leqslant n$. This proves Theorem 2(1).

(2) Proof of Theorem 2(2). By (1) we may assume that n is a square, Our hypothesis implies that the multiplier group has a central involution. Thus, in proving $|M|\leqslant n+1$, we may assume, without loss of generality, that M contains an involution α. Since M is abelian, M induces a group of multipliers on the Baer subplane $B=C_S(\alpha)$. Let K be the kernel of this action. Let P be a point in $A=[S,\alpha]$. Since B is a Baer subplane, P is incident with a line l of B. Therefore $P^K\subseteq l$ as $l^K=l$. Since A is an arc by Theorem 1, this implies that $|P^K|\leqslant 2$. On the other hand, we have $C_A(k)=1$ for all $1\neq k\in K$ as B is a Baer subplane and $A\cap B=1$ by Theorem 1. So $|K|=|P^K|\leqslant 2$.

By (1) and induction, $|M/K|\leqslant\sqrt{n}+1$ except in the case $\sqrt{n}=4$. Suppose $\sqrt{n}=4$. Then $|M/K|\leqslant 6$. Hence, $|M|\leqslant 2\cdot 6\leqslant 17=16+1$. Theorem 2(2) holds in this case. Assume $\sqrt{n}\neq 4$. Then $|M|\leqslant 2(\sqrt{n}+1)$. If $2(\sqrt{n}+1)>n+1$, then $0>n-2\sqrt{n}-1=(\sqrt{n}-1)^2-2$. Thus, $\sqrt{2}>\sqrt{n}-1$. So $n<2+1+2\sqrt{2}=5.8284$. Thus $n\leqslant 5$. However n is a square. Hence, $n=4$. This completes the proof of Theorem 2(2).

(3) Proof of Theorem 2(3). It suffices to verify that the hypothesis in Theorem 2(2) holds. Let t^2 be the order of a projective plane with an abelian Singer group. Theorem 3.1 and Lemma 3.2 imply that the multiplier $m(\sqrt{t^3})$ is a central involution of the multiplier group.

4. THEOREM 3.

We continue to use the notations in Section 2. Let D be a difference set of the Singer group S which is invariant under M. Assume in addition that S is cyclic. Hence, M is abelian. The first part of Theorem 3(1) follows directly from Theorem 2. We remark that this can also be obtained from the following result.

THEOREM 4.1 (Cohen [C]). *With the exception of the two* (21,5,1)*-difference sets, every cyclic* (v, k, λ)*-difference set contains a residue co-prime with* v.

The second conclusion of Theorem 3(1) follows from Proposition 2.5.

4.1. LEMMA. *If* $|M| = n$ *or* $n+1$, *then* $|M|$ *is odd and* $C_S(\alpha) = 1$ *for* $1 \neq \alpha \in M$.

Proof. From $|M| \leqslant n+1$, we may assume M is the multiplier group of Π as $|M| = n$ or $n+1$. The multiplier group has order 6 when $n = 4$. Hence, $n \neq 4$. Let E be any line fixed by M. By Theorem 4.1, E contains a generator e of S. Hence, $M_e = 1$ and so $|e^M| = |M : M_e| = |M| = n$ or $n+1$. This implies that $|C_E(\alpha)| \leqslant 1$. Therefore, E carries at most one fixed point of α. Hence, α cannot be planar. In particular, $|C_S(\alpha)| = 1$ or 3 as v is odd. Since any involution in M is Baer, $|M|$ is odd. Suppose $T = C_S(\alpha)$ has order 3. Then T is the Sylow 3-subgroup of S. Since M has an odd order, this implies that $T \subseteq C_S(M)$. Let l be a line incident with two points in T. Then l is M invariant and $|C_l(M)| \geqslant 2$. However, this contradicts $|C_l(M)| \leqslant 1$, and this contradiction establishes $C_S(\alpha) = 1$.

4.2. LEMMA. *If* $|M| = n$ *or* $n+1$, *then* $v = v(n)$ *is a prime.*

Proof. Let p be a prime dividing v. Then M leaves invariant a subgroup of order p of S as S is cyclic. By Lemma 4.1, we infer that $|M|$ divides $p-1$. So $n \leqslant |M| \leqslant p-1$. Hence, $n+1 \leqslant p$. If there is another prime q diving v, then $n+1 \leqslant q$, also. But this will imply that $v = v(n) < (n+1)^2 \leqslant pq$. This contradiction proves that $v = p^a$ for some $a \geqslant 1$. If $a > 1$, then $p^2 \leqslant p^a = v < (n+1)^2 \leqslant p^2$, again a contradiction. Hence, $v = p$ is a prime.

We now complete the proof of (2) and (3) of Theorem 3. Suppose $|M| = n$. As 3 divides $|M|$ by Theorem 3.1, 3 divides n. Since $|M|$ is odd by Lemma 4.1, so is n. Next, suppose $|M| = n+1$. Then n is even as $|M|$ is odd by Lemma 4.1. The rest of the proof follows from Lemma 4.2.

We now prove Theorem 3(4).

4.3. LEMMA $|M| = n-1$ *if and only if* $n = 2$.

Proof. Suppose $|M| = n-1$ and $n \neq 2$. The order of the multiplier group is at most $n+1$. Assume the multiplier group has order $n+1$, then as $n+1 = n-1+2$, Lagrange theorem implies that $n-1$ divides 2. Hence $n = 2$ or 3. But the multiplier group of a plane of order 3 has order 3 not $n+1 = 4$. Therefore, the multiplier group cannot have order $n+1$ in the present case. Hence, the multiplier group has order n. Thus we may assume that M is the multiplier group. By Hall's multiplier theorem (Theorem 3.1), 3 divides $|M|$. So $n \equiv 1 \pmod 3$. Thus 3 divides v and the Sylow 3-subgroup T of S has order 3. Also, the multiplier $m(n)$ fixes exactly $(n-1, 3) = 3$ points [B]. So $C_S(m(n)) = T$. If all three points of T are collinear with a line l, the $m(n)$ will act fixed-point-freely on the points of l different from T. This implies that 3 divides $n+1-3 = n-2$. This contradiction proves that $T = P(m(n))$ is a triangle. If $n = 4$, then $|M| = 6 \neq 4-1$. Therefore, $n \neq 4$.

Note that D is a side of the triangle T. The two points of T on D are not generators of S as they generate $T < S$. By Theorem 4.1, D contains a generator d of S. So $d \in D \setminus T$. Thus $|d^M| = |M : M_d| = n-1$ implies that $d^M = D \setminus T$. Since M is abelian, this shows that $|C_D(\alpha)| \leqslant 2$ for all $1 \neq \alpha \in M$. This proves that α cannot be planar. In particular, M does not contain any involution and so $|M|$ is odd. Hence, $n = |M| + 1$ is even. So 2 is a multiplier. Therefore n is a square by Lemma 2.6. But this implies that $|M|$ is even. This contradiction proves Lemma 4.3.

We now prove Theorem 3(5).

4.4. LEMMA. $|M| = n-2$ *if and only if* $n = 3$ *or* 5. *In particular,* $n = 5$ *if and only if* $1 \neq M$ *has order* $n-2$. (*In this case* M *is the multiplier group.*)

Proof. If $n = 3$ or 5, then the corresponding multiplier group has order 3, which has a subgroup of order $n-2$.

Assume $|M| = n-2$. Suppose M is a proper subgroup of the multiplier group N. Clearly, $|M| = 1$ if and only if $n = 3$. Assume $1 \neq M$. Since $n-2 \nmid n-1$, $|N| \neq n-1$. If $|N| = n$, then $n \equiv 2 \pmod{n-2}$ implies that $n-2$ divides 2 by Lagrange theorem. So $n = 4$ as $1 \neq M$. But $|N| = 6 \neq 4$ in this case. Hence, $|N| \neq n$. By Theorem 3(1), $|N| = n+1$. As $n+1 \equiv 3 \pmod{n-2}$, this implies that $n-2$ divides 3, and so $n-5$. But $M = N$ in this case. This contradiction proves that if M is not the multiplier group, then $|M| = n-2$ if and only if $M = 1$ and $n = 3$.

We may assume that M is the multiplier group. By Theorem 3.1, 3 divides $|M| = n-2$. So $n \equiv 2 \pmod 3$ and $v \equiv 1 \pmod 3$. So $n \neq 4$ and the Sylow 3-subgroup of S has order 1. Hence, the multiplier $m(n)$ acts fixed-point-freely on D. Since $n \neq 4$, Theorem 4.1 implies that D contains a

generator d of S. Let $\Omega = d^M$. Then $|\Omega| = |M : M_d| = |M| = n-2$. Hence, $D = \Omega \cup \Delta$, where $|\Delta| = 3$ and Δ is an orbit of M by the action of $m((n))$. Since M is abelian, M induces a cyclic group of order 3 on Ω. Let K be the kernel of the action of M on Δ. Then $K \cap \langle m(n) \rangle = 1$ and $M = K \times \langle m(n) \rangle$. Since M acts fixed-point-freely on Ω, K consists of elements of M which have some fixed points in D. Note that these fixed points in D lie in Δ. If $1 \neq \beta \in M$ with $C_S(\beta) \neq 1$, then β is planar as $C_S(\beta)$ is a subgroup and the Sylow 3-subgroup of S is 1. Thus, β has fixed points in D as $m(n)$ acts fixed-point-freely. This implies that $\beta \in K$.

Let $1 \neq \alpha \in K$. Then $\Omega \subseteq C_S(\alpha)$. So $|C_S(\alpha)| > 3$ as the Sylow 3-subgroup of S has order 1. Hence, α is planar. Since D is a line fixed by α and D contains exactly three fixed points of α, $C_S(\alpha)$ is a subplane of order 2. If M has an even order, then the involution belongs to K. This will imply $n = 4$, a contradiction. This contradiction proves that $|M|$ is odd.

If $K = 1$, then $|M| = 3$ and $n = 5$. Hence, we may assume that $K \neq 1$. Since $|C_S(\alpha)| = 7$ for all $1 \neq \alpha \in K$ and S is cyclic, $C_S(\alpha) = C_S(K)$ is the subgroup of order 7 of S. Suppose $v = |S| = 7$. Then $n = 2$ and $|M| = 0$. This contradiction proves that $v > 7$.

Assume $p \neq 7$ is a prime divisor of v. Since $5 \nmid v$ and $3 \nmid v$ in the present case, we have $p > 7$. Thus M acts fixed-point-freely on the cyclic subgroup of order p of S. This implies $n-2 = |M|$ divides $p-1$. In particular, $n-2 \leqslant p-1$. So $n-1 \leqslant p$. If there is another prime $q \neq 7$ such that $q \mid v$, then we may assume without loss of generality that $q > p$. Since v is odd, so p and q are both odd. Hence, $q > p+1 \geqslant n$. This implies that $v \leqslant (p+1)^2 + (p+1) + 1 = p^2 + 3p + 3$. However, $v \geqslant 7pq \geqslant 7p(p+2) = 7p^2 + 14p$. We now obtain a contradiction, namely, $7p^2 + 14p \leqslant p^2 + 3p + 3$ (i.e. $6p^2 + 11p \leqslant 3$). This proves that there exists at most one prime different 7 dividing v. Similarly, if $p^2 \mid v$, then we have $p^2 + 3p + 3 \geqslant v \geqslant 7p^2$. So $3(p+1) \geqslant 6p^2$ or $p + 1 \geqslant 2p^2$. This contradiction proves that $v = 7^a p$. Since M acts fixed-point-freely on the Sylow p-subgroup of S, M is a Frobenius complement. As M is abelian, so M is cyclic. From $M = K \times \langle m(n) \rangle$, we infer that K has order prime to 3.

Let $K = \langle k \rangle$. Let W be the Sylow 7-subgroup of S. Now $C_S(k) = \Omega_1(W)$, the subgroup of order 7 in W. This implies that the order of k is a power of 7. Let the order of k be 7^b. Then $|M| = 3 \cdot 7^b = n-2$. Hence, $n = 3 \cdot 7^b + 2$, and so $v = (9 \cdot 7^{2b} + 4 \cdot 3 \cdot 7^b + 4) + (3 \cdot 7^b + 2) + 1 = 9 \cdot 7^{2b} + 15 \cdot 7^b + 7 = 7(9 \cdot 7^{2b-1} + 15 \cdot 7^{b-1} + 1)$.

If $b = 1$, then $n = 3 \cdot 7 + 2 = 23$. But then $|M| \neq n-2$. Hence, $b > 1$. Thus, $c = 9 \cdot 7^{2b-1} + 15 \cdot 7^{b-1} + 1 \equiv 1 \pmod 7$. From $v = 7^a p = 7c$, we have $p = c$ and $a = 1$. Now $p - 1 = 7^{b-1}(9 \cdot 7^b + 15)$. Since $3 \cdot 7^b = |M| \mid (p-1)$, we have $3 \cdot 7 \mid 9 \cdot 7^b + 15$. So $7 \mid 9 \cdot 7^b + 15 \equiv 1 \pmod 7$. This contradiction proves that $v = 7^a$. But $|M| = 3 \cdot 7^b$ implies that $v = 7c$ with $c \equiv 1 \pmod 7$. This contradiction proves that $K = 1$ and thus completes the proof.

We now prove Theorem 3(6).

4.5. LEMMA. *$|M| = n-3$ if and only if $n=4$ or 9. In particular, $n=9$ if and only if $1 \neq M$ has order $n-3$.*

Proof. If $n=4$ or 9, then the corresponding multiplier group has order 6 or 9, which has a subgroup of order $n-3$.

Assume $|M| = n-3$. Suppose M is a proper subgroup of the multiplier group N. Clearly $|M| = 1$ if and only if $n=4$. Assume $1 \neq M$. By Theorem 3(4), the possibilities for $|N|$ are $n-2$, n, $n+1$. Using Lagrange theorem, the corresponding possibilities for n are respectively 4, 6, and 7. Since the plane of order 6 does not exist and for the plane or order 7, $|N| = 3$ not $7+1$, so the situation $1 < M < N$ cannot occur. Therefore, we may assume M is the multiplier group. By Theorem 3.1, $n \equiv 0 \pmod 3$. This implies that n is odd [L, p. 206]. Hence, $|M| = n-3$ is even. Let i be the involution in M. Then $P(i) = C_S(i)$ is a Baer subplane and D is a line of this subplane. By Theorem 4.1, D contains a generator d of S. Hence $|d^M| = |M| = n-3$. As M acts fixed-point-freely on d^M, the fixed points for i belong to $D \backslash d^M$, which has four points. Therefore, $\sqrt{n} \leqslant 4-1$. Since n is odd, this implies that $\sqrt{n} = 3$ and $n=9$ as desired.

5. REMARKS ON CYCLIC PLANES

In this section, projective planes are cyclic planes of order n, $v = n^2+n+1$, and M is a group of multipliers.

(5.1) If v is a prime, then certainly $|M|$ divides n or $n+1$. Theorem 3 proves that if $|M| = n$ or $n+1$, then v is a prime. For the Desarguesian plane of order 27, the multiplier group has order 9 dividing 27, and $v(27) = 757$ is a prime. However, for the Desarguesian plane of order 3^9, the multiplier group has order 27 dividing 3^9. But $v(3^9) = 387440173$ is divisible by 109. Also for the Desarguesian plane of order 125, the multiplier group has order 9 which divides $125+1$, but $v(125) = 15751 = 19 \times 829$.

(5.2) In the proof of (2) and (3) of Theorem 3, the fact that M does not contain planar elements has been used to show that v is a prime. The Desarguasian plane of order 125 (or 7^3) shows the condition that M does not contain any planar element is not sufficient for v to be a prime.

(5.3) Suppose the group M of multipliers does not contain any planar element. If $|M| > (n+1)/2$, then $|M| = n+1$ or n.

Proof. By Proposition 2.5, we have $|M| = 3s \mid |\Omega| = n-j = 3t$. Hence, $s = t$ or $2s \leqslant t$. Assume $s < t$. Then $n+1 = 2|M| < 2(3s) = 3(2s) \leqslant 3t = n-j$.

This contradiction proves that $s = t$. Now the result follows from (2), (3), and (4) of Theorem 3.

A corollary of (5.3) is the following.

(5.4) Suppose M does not contain any planar element. If $|M| = n - k$ for some $k \geqslant 1$, then $n \leqslant 2k + 1$.

Proof. By Theorem 3(4), we may assume $k > 1$. By (5.3), we have $n - k = |M| \leqslant (n+1)/2$. This implies $n \leqslant 2k + 1$.

In [Ho], it is proved that if $|M| = 3$, then n is a prime. On the other hand, (5.4) treats the case when $|M|$ is relatively big with respect to n (i.e., k is small). An easy computation shows the following.

(5.5) If $1 \leqslant k \leqslant 10$ in (5.4), then $k = 2$, 4, 8, 10, and the corresponding value of n is 5, 7, 11, and 13.

REFERENCES

[D] P. DEMBOWSKI, "Finite Geometries," Springer-Verlag, New York, 1968.

[B] L. D. BAUMERT, "Cyclic Difference Sets," Lecture Notes in Math., Vol. 182, Springer-Verlag, New York, 1971.

[C] S. D. COHEN, Generators in cyclic difference sets, *J. Combin. Theory Ser. A* **51** (1989), 227–236.

[F] W. FEIT, Finite projective planes and a question about primes, *Proc. Amer. Math. Soc.* **108** (1990), 561–564.

[FT] W. FEIT AND J. THOMPSON, Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775–1029.

[G] D. GORENSTEIN, "Finite groups," Harper & Row, New York, 1968.

[Ho] C. Y. HO, On multiplier groups of finite cyclic planes, *J. Algebra* **122** (1989), 250–259.

[Ho1] C. Y. HO, Some remarks on order of projective planes, planar difference sets and multipliers, *Designs, Codes and Crytography* **1** (1991), 69–75.

[HoP] C. Y. HO AND A. POTT, On multiplier groups of planar difference sets and a theorem of Kantor, *Proc. Amer. Math. Soc.* **103** (1990), 803–808.

[H-P] D. HUGES AND F. PIPER, "Projective Planes," Springer-Verlag, New York, 1973.

[K] W. M. KANTOR, Primitive permutation groups of odd order and an application to finite projective planes, *J. Algebra* **106** (1987), 15–45.

[L] E. S. LANDER, "Symmetric Designs: An Algebraic Approach," London Math. Soc. Lecture Note Series. Vol. 74, Cambridge Univ. Press, London, 1983.

[O] OTT, Endliche zyklische Ebenen, *Math. Z.* **144** (1975), 195–215.